PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-057097
(43)Date of publication of application : 25.02.2000

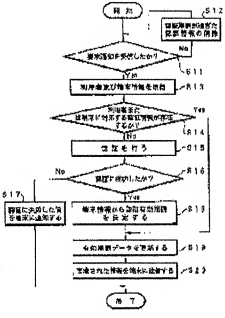
(51)Int.Cl. G06F 15/00
G06F 13/00

(21)Application number : 10-228749
(22)Date of filing : 13.08.1998

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : SATAKE MASAKI

(54) IMAGE PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To keep the security of a service to be provided without damaging operability on the side of an external device by automatically determining the validity of certification corresponding to the characteristics (environment or performance) of the external device to access an image processor for providing the image processing service.
SOLUTION: Concerning this image processor, when a processing request from the external device is accepted (S11), information related to the issue source of that processing request is acquired (S13) and certification is performed based on the acquired information (S15). At such a time the validity of that certification is determined and corresponding to the acquired information, the length of validity to be determined is changed (S18). When that certification is valid, only within the validity, prescribed processing corresponding to the accepted processing request is executed (S20).



(TRANSLATION)

Our Ref.: OP1710-US

Prior Art Document:

Japanese Patent Laid-Open Publication No. 2000-57097

Laid-Open Date: February 25, 2000

Patent Application No. 10(1998)-228749

Filing Date: August 13, 1998

Applicant: 000005496
FUJI XEROX KABUSHIKI KAISHA
(English: FUJI XEROX CO LTD.)
Minato-ku, Tokyo, Japan

Inventor: Masaki SATAKE
c/o EBINA BRANCH OF FUJI XEROX CO LTD.
Ebina-shi, Kanagawa-ken, Japan

Title of the Invention: IMAGE PROCESSOR

- -

PARTIAL TRANSLATION: Paragraphs [0031]-[0032] and [FIG. 1]

[0031]

As exemplified in the drawings, when the WWW server 1 becomes in the operable state by throw-in of the power source, it is, from that point of time, in a state of waiting for an information providing request. Then, after the lapse of a predetermined period of time (for example, one second) in that state, at the WWW server 1, the CPU 4 determines whether there is the information providing request or not (step 11, hereinafter the step will be called "S"). Namely, the CPU 4 determines whether the request for providing the information has been received from the user terminal through the network interface 3, or not.

[0032]

Here, when there is no receipt of the request, then subsequently, the CPU 4 compares the time information at that time, which is notified from the system clock 8, with the "authentication validity term" of each entry (each line in the right side column of the table in Fig. 4) of the authentication term data stored in the HDD 7, and determines whether there is the "authentication validity term" which has already elapsed the aforementioned time information. Then, when there is the "authentication validity term" which has already elapsed, the whole entry including the "authentication validity term" is deleted from the HDD 7 (S12). Thereafter, the CPU 4 resumes the state of waiting for the information providing request, and repeats the above-mentioned steps (S11-S12).

- -

[FIG. 1]

START-UP

S11 . . . Has the request notice been received?

S12 . . . Deletion of the authentication information which has elapsed the authentication term

S13 . . . Acquiring the user and terminal information

S14 . . . Is the authentication information, which corresponds to the user or the terminal, exists?

S15 . . . Performs authentication

S16 . . . Has the authentication been successful?

S17 . . . Notifies the terminal of failure in authentication

S18 . . . Determines the authentication validity term from
the terminal information

S19 . . . Updates the validity term data

S20 . . . Transmits the requested information to the terminal

END

/ / / / / / / / / / LAST ITEM / / / / / / / / / / / / / /

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－57097
（P2000－57097A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０８５
13/00	３５１	13/00	３５１Ｚ	５Ｂ０８９

審査請求　未請求　請求項の数４　ＯＬ　（全８頁）

(21)出願番号　特願平10－228749

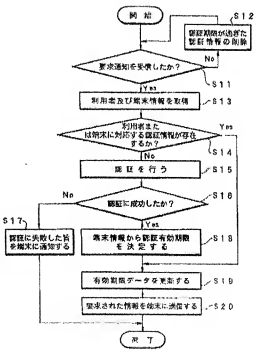
(22)出願日　平成10年８月13日(1998.8.13)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　佐竹　祥紀
神奈川県海老名市本郷2274番地　富士ゼロックス株式会社海老名事業所内
(74)代理人　100086298
弁理士　船橋　國則

Ｆターム(参考)　５Ｂ０８５ Ａ００３ Ａ００１ Ａ２３ Ｂ００７
５Ｂ０８９ Ｇ０１１ Ｊ０２１ Ｋ０１７ Ｋ０１３
Ｋ０３４ Ｋ０５８

(54)【発明の名称】　画像処理装置

(57)【要約】
【課題】　画像処理サービスを提供する画像処理装置において、これにアクセスする外部装置の特性（環境や性能等）に応じて認証の有効期間を自動的に決定することで、外部装置側での操作性を損なうことなく、提供するサービスのセキュリティを確保する。
【解決手段】　画像処理装置において、外部装置からの処理要求を受け付けると（Ｓ１１）、その処理要求の発行元に関する情報を取得し（Ｓ１３）、取得した情報を基に認証を行う（Ｓ１５）。このとき、その認証の有効期間を決定するとともに前記取得した情報に応じて決定すべき有効期間の長さを変化させる（Ｓ１８）。そして、その認証が有効で、かつ、有効期間内である場合にのみ、受け付けた処理要求に応じた所定処理を実行する（Ｓ２０）。



1

【特許請求の範囲】

【請求項１】　所定の処理を実行する処理手段と、

前記処理手段に対する外部装置からの処理要求を受け付ける要求受付手段と、

前記要求受付手段が処理要求を受け付けると該処理要求の発行元である外部装置に関する情報を取得する情報取得手段と、

前記情報取得手段が取得した情報を基に前記要求受付手段が受け付けた処理要求による処理を前記処理手段に実行させるか否かを判断する認証手段と、

前記認証手段による判断の有効期間を決定するとともに前記情報取得手段が取得した情報に応じて決定すべき有効期間の長さを変化させる期間決定手段とを備えることを特徴とする画像処理装置。

【請求項２】　前記情報取得手段が取得する情報は、前記外部装置を識別するためのアドレス情報であることを特徴とする請求項１記載の画像処理装置。

【請求項３】　前記情報取得手段が取得する情報は、前記外部装置を操作する操作者を識別するための操作者名であることを特徴とする請求項１記載の画像処理装置。

【請求項４】　前記要求受付手段による処理要求の受け付けが前記期間決定手段により決定された有効期間の経過後であった場合に、当該処理要求の発行元である外部装置に対してその旨を通知する通信制御手段が設けられていることを特徴とする請求項１，２または３記載の画像処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク化された環境において用いられるもので、例えば画像情報を含む各種情報の提供や画像のプリントサービスといった画像処理サービスをネットワーク上の他の装置に提供する画像処理装置に係わり、特に画像処理サービスの提供にあたってその要求元についての認証を行う画像処理装置に関するものである。

【０００２】

【従来の技術】一般に、ファイル共有サーバやプリントサーバ等のように画像処理サービスを提供する画像処理装置においては、サービスの提供を特定の利用者のみに制限したり、サービスの利用率を調整（加減）するために、利用要求に対する認証処理を行うものがある。例えば、ハイパーテキスト等を用いて画像情報を含む各種情報の提供サービスを行うことで知られるWWW（World Wide Web）サーバでは、認証処理を行って利用者を特定することで、不正なアクセスを防止するようになっている。

【０００３】このような画像処理装置、特にWWWサーバでは、認証処理を行うのに際し、利用者が操作する端末装置（以下、利用者端末と称す）との間における情報符号化方法および情報伝達方法として、利用者の個人情報（例えば操作者名およびパスワード）を授受することで情報閲覧の可否を決定するＢＡＳＩＣ認証や、ＢＡＳＩＣ認証の場合に加えて授受する個人情報に暗号化を行うＭＤ５認証等を利用しているものが多い。

2

【０００４】また、近年では、提供すべき情報の更なるセキュリティ向上を図るために、ＢＡＳＩＣ認証やＭＤ５認証等の一般的な認証処理とは異なり、独自の方法に従って認証処理を行うものもある。例えば、特開平９－１４６８２４号公報には、利用者端末からWWWサーバへの初回アクセスの成功時（このときはＢＡＳＩＣ認証やＭＤ５認証等による）に、ある特定のＵＲＬ（Uniform Resource Locator）を有効期限が設定された認証識別子として利用者端末に通知し、次回以降のアクセス時に利用者端末がその認証識別子を使用すると、WWWサーバがその認証識別子および認証識別子の有効期限を基に情報閲覧の可否を決定することが開示されている。この認証方法によれば、認証識別子に有効期限が設定されているので、その認証識別子によるアクセス可能期間が制限されることとなり、認証識別子が漏洩した場合であっても不正なアクセスを有効に防止できるようになる。

【０００５】

【発明が解決しようとする課題】ところで、上述した従来の技術においては、認証処理の結果に有効期限を設定することで提供すべき情報の更なるセキュリティ向上を図っているが、その有効期限、すなわち一旦認証された利用者が継続して情報を閲覧し得る期間が、WWWサーバと利用者端末との環境条件に拘わらず一律に設定される。例えば、WWWサーバと同一ネットワーク上に存在する利用者端末からのアクセスであっても、WWWサーバとは異なるネットワーク上の利用者端末または公衆電話回線網を経由した外部の利用者端末からのアクセスであっても、その有効期限は共に同一である。

【０００６】換言すると、不正アクセスの可能性が低い利用者端末（または利用者）およびその可能性が高い利用者端末（または利用者）のいずれにおいても、認証処理の結果に対する有効期限は、同一に設定されてしまう。したがって、不正なアクセスを有効に防止するためには、有効期限を短く設定することが考えられる。

【０００７】しかしながら、認証処理の結果に対する有効期限を短くすると、正当に認証を受けた利用者端末（または利用者）が情報の閲覧を継続する場合であっても、初回アクセスに担当するＢＡＳＩＣ認証やＭＤ５認証等のために、個人情報の送信を度々要求することになってしまう。よって、利用者端末側では処理効率の低下を招いてしまうとともに、操作性が損なわれてしまい、利用者にとっても非常に煩わしいものとなってしまうおそれがある。これに対して、認証処理の結果に対する有効期限を長くすれば、利用者端末側での操作性を改善することもできるが、この場合には、不正アクセスの可能性が高い利用者端末（または利用者）に対しても長期間

の情報閲覧を許すこととなり、結果としてセキュリティの低下を招いてしまうおそれがある。

【０００８】そこで、本発明は、認証処理によって特定された利用者に対して情報閲覧等の画像処理サービスを提供する画像処理装置において、これにアクセスする各利用者端末の特性（環境や性能等）に応じて認証の有効期間を自動的に決定することで、利用者端末側での操作性を損なうことなく、提供するサービスのセキュリティを確保することのできる画像処理装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】本発明は、上記目的を達成するために案出された画像処理装置で、所定の処理を実行する処理手段と、前記処理手段に対する外部装置からの処理要求を受け付ける要求受付手段と、前記要求受付手段が処理要求を受け付けるとその処理要求の発行元である外部装置に関する情報を取得する情報取得手段と、前記情報取得手段が取得した情報を基に前記要求受付手段が受け付けた処理要求による処理を前記処理手段に実行させるか否かを判断する認証手段と、前記認証手段による判断の有効期間を決定するとともに前記情報取得手段が取得した情報に応じて決定すべき有効期間の長さを変化させる期間決定手段とを備えることを特徴とするものである。

【００１０】上記構成の画像処理装置によれば、要求受付手段が外部装置からの処理要求を受け付けると、その処理要求による処理を処理手段に実行させるか否かを認証手段が判断する。ただし、このとき、期間決定手段では、認証手段による判断の有効期間を決定するとともに、情報取得手段が取得した外部装置に関する情報に応じて決定すべき有効期間の長さを変化させる。したがって、この画像処理装置では、例えばある外部装置からの処理要求に対する認証についてはその有効期間を長くし、他の外部装置からのものについては有効期間を短くする、といったことが可能となる。つまり、処理要求の発行元に応じた認証の重み付けができるようになる。

【００１１】

【発明の実施の形態】以下、図面に基づき本発明に係わる画像処理装置について説明する。ただし、ここでは、本発明を、画像情報を含む各種情報の提供サービスを行うWWWサーバに適用した場合を例に挙げて説明する。図１は、本発明を適用したWWWサーバにおける認証処理の手順を示すフローチャートであり、図２は、その認証処理を行うWWWサーバの概略構成の一例を示すブロック図である。

【００１２】図２に示すように、本実施の形態におけるWWWサーバ１は、例えばインターネットと呼ばれるＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）ネットワーク２に接続されており、このネットワーク２上に存在する利用者端末（ただし不図示）からの処理要求に応じて、各種情報の提供サービスを行うものである。

【００１３】このネットワーク２上に存在する利用者端末は、WWWブラウザが動作可能なパーソナルコンピュータ（ＰＣ）やワークステーション（ＷＳ）等からなるもので、そのWWWブラウザの動作によってＲＦＣ１９４５で規定されたＨＴＴＰ（Hyper Text Transfer Protocol）／１．０に従った通信を行い、WWWサーバ１に対してハイパーテキストや画像情報等の提供を要求するとともに、提供を受けた各種情報を利用者の閲覧のためにディスプレイ上に表示するものである。

【００１４】このような利用者端末への情報提供サービスを行うために、WWWサーバ１は、ネットワークインタフェース３と、ＣＰＵ（Central Processing Unit）４と、ＲＯＭ（Read Only Memory）５と、ＲＡＭ（Random Access Memory）６と、ハードディスク装置（以下、ＨＤＤと略す）７と、システム時計８と、これらを互いに接続するシステムバス９とを備えて構成されている。

【００１５】ネットワークインタフェース３は、ネットワーク２と接続するためのもので、ＴＣＰ／ＩＰおよびＨＴＴＰ／１．０に準拠した通信およびその制御を行うためのものである。なお、ネットワークインタフェース３は、複数のネットワーク２のそれぞれと同時に接続しているものであってもよい。

【００１６】ＣＰＵ４は、WWWサーバ１全体の動作制御を行うものである。さらに詳しくは、利用者端末への情報送信処理や、詳細を後述する有効期限の算出処理を含んだ認証処理など、情報提供サービスの実現に必要な処理を行うものである。

【００１７】ＲＯＭ５は、ＣＰＵ４による動作制御に必要な制御プログラムを予め格納しているものである。このＲＯＭ５が格納する制御プログラムとしては、例えばＣＰＵ４がプロトコルＨＴＴＰ／１．０に従いネットワークインタフェース３を介して利用者端末に各種情報を送信するためのものがある。ＲＡＭ６は、ＣＰＵ４のワークエリアとして用いられるもので、プログラム制御変数や各種処理のためのデータ等を格納するためのものである。

【００１８】ＨＤＤ７は、大容量を有した不揮発性の記憶装置であり、利用者端末に提供すべき画像情報を含む各種情報を記憶しているものである。また、ＨＤＤ７には、これに加えて、ＣＰＵ４が認証処理を行う際に参照する利用者データと、利用者端末からの処理要求を実行するか否かを決定する際に参照する認証期限データと、が格納されている。なお、ＨＤＤ７は、不揮発性のものであれば他の記憶装置からなるものであってもよい。

【００１９】ここで、ＨＤＤ７に格納される利用者データおよび認証期限データについて、さらに詳しく説明する。

5

【００２０】利用者データとは、図３に示すように、利用者を識別するための「操作者名」と、各利用者毎に個別に与えられた「パスワード」とが、各種情報の提供を許可し得る利用者毎にテーブル化された情報である。すなわち、利用者データは、ＣＰＵ４に認証され得る利用者についての個人情報に相当するものである。なお、利用者データは、ＷＷＷサーバ１の管理者等の操作によって、ＨＤＤ７内に事前に格納されているものとする。

【００２１】認証期限データは、図４に示すように、利用者を識別するための「操作者名」と、その利用者が操作する利用者端末に個別に付された「ＩＰ（Internet Protocol）アドレス」と、認証処理の結果に対する有効期限を表す「認証有効期限」とが、利用者データの場合と同様にテーブル化されたものである。ただし、この認証期限データは、利用者データとは異なり、ＣＰＵ４からの指示に従ってその登録または削除が行われるようになっている。

【００２２】また図２において、システム時計８は、時計用チップにより構成されたもので、時刻情報（年月日、時分秒等）をＣＰＵ４に通知するためのものである。なお、システム時計８は、システム電源断時や停電時等に時刻情報が消滅しないようにバックアップ用電池を備えており、常に現在時刻を計時しているものとする。

【００２３】次に、以上のように構成されたＷＷＷサーバ１において、利用者端末からの処理要求に対して認証処理を行う場合の動作例について説明する。ただし、ここでは、ＷＷＷサーバ１が利用者端末との間の情報符号化方法および情報伝達方法として、ＢＡＳＩＣ認証を利用している場合を例に挙げて説明する。

【００２４】先ず、ここで、このＷＷＷサーバ１におけるＢＡＳＩＣ認証の基本的な手順について説明する。図５は、ＷＷＷサーバ１がＢＡＳＩＣ認証を行った際の、ＷＷＷサーバ１と利用者端末との間のデータ授受を簡単に示した図である。

【００２５】ＷＷＷサーバ１に対して情報提供を要求する場合に、利用者端末側では、そのＷＷＷサーバ１に対して要求情報を指し示すＵＲＬを送信し、情報提供の要求を行う（図中①参照）。具体的には、図６のようなデータ列を送信して、情報の提供を要求する。

【００２６】一方、ＷＷＷサーバ１では、利用者端末からのＵＲＬを受信するとと、そのＵＲＬによって要求された情報が認証を必要とするものであるか否かを判断し、認証が必要であればその旨および認証のために必要なパラメータに関するデータを利用者端末に返信する（図５中②参照）。具体的には、図７のようなデータ列（応答コード４０１）を返信する。

【００２７】これに対して、利用者端末側では、ＷＷＷサーバ１から受け取ったデータ内のパラメータに従って、利用者の個人情報（操作者名およびパスワード）を

6

ＷＷＷサーバ１に通知する（図５中③参照）。具体的には、図８のようなデータ列を通知する。

【００２８】そして、ＷＷＷサーバ１は、利用者端末側からの個人情報を受け取った後に、その個人情報をＨＤＤ７内の利用者データと比較して、利用者端末側の利用者についての認証を行う。このとき、個人情報が利用者データと一致すれば、ＷＷＷサーバ１は、その利用者による情報閲覧を許可することを決定し、ＵＲＬによって要求された情報を利用者端末へ送信する（図５中④参照）。具体的には、図９のようなデータ列（応答コード２００）を送信する。また、個人情報と利用者データとが一致しなければ、ＷＷＷサーバ１は、その利用者による情報閲覧を拒否することを決定し、その旨を利用者端末側に通知する（図５中④参照）。具体的には、図１０のようなデータ列（応答コード４０３；「サーバはリクエストを理解したが実行を拒否する」の意）を通知する。

【００２９】なお、ＷＷＷサーバ１と利用者端末との間では、利用者端末から要求された情報が認証を必要としない場合または既に認証済である場合には、図５中の②および③のデータ通知を行わないものとする。

【００３０】続いて、以上のようなＢＡＳＩＣ認証を利用したＷＷＷサーバ１が行う認証処理の詳細な手順について、すなわち本発明の特徴的な点である認証処理の手順について、図１のフローチャートを参照しながら詳しく説明する。なお、以下に説明する認証処理は、ＷＷＷサーバ１への電源投入時から繰り返して行われるものとする。また、ここでは、ＷＷＷサーバ１から利用者端末に対して提供する情報については全て認証を必要とするものとして説明する。

【００３１】図例のように、ＷＷＷサーバ１は、電源投入等により動作可能状態になると、その時点から情報提供要求の待ち状態となる。そして、その状態で所定時間（例えば１秒間）経過すると、ＷＷＷサーバ１では、ＣＰＵ４が情報提供要求の有無を判断する（ステップＳ１１、以下ステップをＳと略す）。すなわち、ＣＰＵ４は、情報提供の要求をネットワークインタフェース３を介して利用者端末から受信したか否かを判断する。

【００３２】ここで、要求の受信が無ければ、続いて、ＣＰＵ４は、システム時計８から通知されるその時点の時刻情報と、ＨＤＤ７内に格納された認証期限データの各エントリ（図４のテーブルにおける各行）の「認証有効期限」とを比較して、既にその時刻情報を経過している「認証有効期限」があるか否かを判断する。そして、既に経過している「認証有効期限」があれば、その「認証有効期限」を含むエントリを、ＨＤＤ７内から削除する（Ｓ１２）。その後、ＣＰＵ４は、再び情報提供要求の待ち状態となり、上述のステップ（Ｓ１１～Ｓ１２）を繰り返す。

【００３３】ただし、利用者端末からの情報提供要求の

受信があると（図５中の①に相当、図６のデータ列参照）、ＣＰＵ４は、その要求発行元の利用者を識別する「操作者名」と、ＴＣＰ／ＩＰ通信時に取得可能でその利用者が操作する利用者端末に付された「ＩＰアドレス」とを、受信した要求の中から抽出して取得し（Ｓ１３）、これらをＲＡＭ６内の所定領域に一時的に格納する。

【００３４】情報提供要求から「操作者名」および「ＩＰアドレス」を取得すると、次いで、ＣＰＵ４は、ＨＤＤ７内に格納されている認証期限データの各エントリを検索して、ＲＡＭ６内に一時的に格納した「操作者名」および「ＩＰアドレス」と一致するエントリが、認証期限データ内に既に存在しているか否かを調べる（Ｓ１４）。

【００３５】このとき、認証期限データ内にエントリが存在していれば、そのエントリは先に述べたステップ（Ｓ１２）で削除されておらず、その利用者および利用者端末の組み合わせに対する認証が有効期限内であるため、ＣＰＵ４は、改めて認証処理（図５中の②、③に相当）を行うことなく、要求された情報をＨＴＴＰ／１．０プロトコルに従いつつネットワークインタフェース３を介して要求元の利用者端末へ送信する（Ｓ２０；図５中の④に相当、図９のデータ列参照）。

【００３６】ただし、認証期限データ内にエントリが存在しなければ、その利用者および利用者端末の組み合わせについては未だ認証処理が行われていないか、あるいは有効期限の経過後であるため、ＣＰＵ４は、その利用者端末との間で先に述べたＢＡＳＩＣ認証（図５中の②、③に相当、図７、８のデータ列参照）を行った後に（Ｓ１５）、その利用者端末に対する情報提供の可否、すなわち認証に成功したか否かを判断する（Ｓ１６）。

【００３７】この判断の結果、認証が成功していなければ情報提供を拒否することになるので、ＣＰＵ４は、情報提供の要求元である利用者端末に対して、認証が失敗した旨を通知する（Ｓ１７）。詳しくは、利用者端末に送信すべき応答データ内に応答コード４０３を記述し（図１０のデータ列参照）、ＨＴＴＰ／１．０に従った通知を行う（図５中の④に相当）。

【００３８】一方、認証が成功した場合には、ＣＰＵ４は、続いて、その認証処理の結果に対する有効期限を決定する（Ｓ１８）。

【００３９】ここで、ＣＰＵ４による有効期限の決定について、図１１の説明図を参照しながら詳しく説明する。

【００４０】ＣＰＵ４が決定する有効期限は、ＨＤＤ７内に格納される認証期限データの「認証有効期限」に相当するもので、以下に述べるような所定の演算によって算出されるものである。すなわち、有効期限は、図中の（１）式に示すように、システム時計８から通知される認証成功時点の時刻情報と有効期間との和によって算出

される。ここでいう有効期間とは、図中の（２）式に示すように、予め所定値に設定された最大有効期間と、後述するように情報提供の要求元である利用者端末の「ＩＰアドレス」に応じて決定される有効期間係数との積によって算出されるものである。なお、最大有効期間としては、例えば図中の（３）式に示すように、１日＝２４時間＝１４４０分といったように設定することが考えられる。

【００４１】ところで、このＷＷＷサーバ１では、ネットワークインタフェース３が接続しているネットワーク２の数に応じて「ＩＰアドレス」が付されている。例えば、ネットワークインタフェース３が三つのネットワーク２と接続していれば、ＷＷＷサーバ１には、一般対象アドレスとして「129.249.010.001 」、「129.249.021.011 」および「128.212.041.008 」といった三種の「ＩＰアドレス」が付されているものとする。

【００４２】このように「ＩＰアドレス」は、具体的には全１２桁の数字列（または文字列）からなるものであるが、そのうちの上位３桁は国単位で値が異なり、次の３桁は企業（団体）単位で値が異なり、さらに次の３桁はサブネットワーク（エリア）単位で値が異なり、下位３桁は装置単位で値が異なるように、それぞれのＷＷＷサーバまたは利用者端末に個別に付されている。

【００４３】このことから、ＣＰＵ４は、ＷＷＷサーバ１に付された「ＩＰアドレス」と、情報提供要求の発行元である利用者端末の「ＩＰアドレス」とを比較して、これらの間で一致する桁数がどれだけあるかを認識し、その認識結果に応じてそれぞれの間の環境条件を判断することによって有効期間係数の値を決定する。例えば、ＣＰＵ４では、互いの「ＩＰアドレス」の間で一致する桁数が多いほど、要求発行元の利用者端末がＷＷＷサーバ１に近い環境にあると判断して、有効期間係数の値が大きくなるように決定する。ただし、「ＩＰアドレス」の一致する桁数と有効期間係数の値との対応関係は、ＣＰＵ４が参照し得るようにＨＤＤ７内の所定領域等に予めテーブル形式で登録されているものとする。

【００４４】つまり、ＣＰＵ４は、先のステップ（図１におけるＳ１３）で取得してＲＡＭ６内に格納した「ＩＰアドレス」をＷＷＷサーバ１の「ＩＰアドレス」と比較することで有効期間係数の値を決定した後に、その有効期間係数および所定値である最大有効期間から有効期間を算出し、さらにはその有効期間をシステム時計８から得られる時刻情報に加えることで、認証処理の結果に対する有効期限を決定するようになっている。

【００４５】このようにして認証結果の有効期限を決定すると、続いて、ＣＰＵ４は、図１に示すように、その有効期限を「認証有効期限」とし、ＨＤＤ７内の認証期限データを更新する（Ｓ１９）。すなわち、ＣＰＵ４は、決定した有効期限を「認証有効期限」とするとともに、これに対応する「操作者名」および「ＩＰアドレ

ス」をＲＡＭ６内から取り出して、これらを一組のエントリとし、その一組のエントリをＨＤＤ７内の認証期限データが登録されたテーブルの最後尾に追加する。

【００４６】その後、ＣＰＵ４は、認証が成功し、かつ、その認証結果の有効期限を決定したことから、先述した認証が有効期限内である場合と同様に、要求された情報を要求元の利用者端末へ送信する（Ｓ２０；図５中の④に相当、図９のデータ列参照）。

【００４７】以上のように、本実施の形態のＷＷＷサーバ１では、認証処理を行うのに際し、その要求元の「ＩＰアドレス」に応じて、ＣＰＵ４が有効期限の長さを変化させるようにしている。これにより、例えばＷＷＷサーバ１に近い環境にある利用者端末については有効期限を長くし、ＷＷＷサーバ１から遠い環境にある利用者端末については有効期限を短くする、といったように要求発行元に応じて認証の重み付けをすることが可能となる。したがって、このＷＷＷサーバ１によれば、例えば遠い環境にある利用者端末に対してはセキュリティを確保しつつ、近い環境にある利用者端末に対しては処理効率や操作性の悪化を防ぐことができるようになる。つまり、各利用者端末の特性（環境や性能等）に応じて認証期限を自動的に決定し、認証期限を経過した利用者端末からのアクセスを拒否することで、不正アクセスの防止と利用者端末側での操作性向上との双方を共に実現できるようになる。

【００４８】また、本実施の形態のＷＷＷサーバ１では、認証期限内であれば改めて認証処理を行うことなく情報の閲覧を許可するが、認証期限内であるか否か、すなわち認証期限データ内にエントリが存在しているか否かを「操作者名」および「ＩＰアドレス」を基に判断するようになっている。つまり、利用者および利用者端末の組み合わせに対する認証が有効期限内であるか否かを判断するため、例えば一旦認証された利用者端末であっても第三者が使用した場合には再び認証処理が必要となる。したがって、このＷＷＷサーバ１によれば、「操作者名」および「ＩＰアドレス」を基にすることにより情報要求元の特性（環境や性能、端末を操作する利用者等）をより確実に判断できるとともに、これらを基に認証処理の要否を判断することによりセキュリティ確保が確実なものとなる。

【００４９】さらに、本実施の形態のＷＷＷサーバ１では、認証期限の経過後に利用者端末からのアクセスがあると、その旨を利用者端末に対して通知するようになっているため、利用者側においては再認証が必要なことを容易に認識することができ、利用者にとって非常に便利なものとなる。

【００５０】なお、本実施の形態では、各種情報の提供サービスを行うＷＷＷサーバに本発明を適用した場合を例に挙げて説明したが、本発明はこれに限定されるものではなく、ネットワーク上の利用者端末に画像処理サービスを提供するものであれば、例えばファイル共有サーバやプリントサーバ等の画像処理装置であっても適用可能である。

【００５１】また、本実施の形態では、利用者端末の「ＩＰアドレス」に応じてＣＰＵ４が有効期限の長さを変化させる場合を例に挙げて説明したが、各利用者端末の特性（環境や性能等）を特定できる情報であれば他の情報を用いてもよい。

【００５２】さらに、本実施の形態では、ＣＰＵ４が有効期限の長さを変化させるのにあたって予め登録された有効期間係数を用いる場合を例に挙げて説明したが、この有効期間係数あるいは「ＩＰアドレス」と有効期間係数との対応関係等は、ＷＷＷサーバ１の管理者等によって任意に選択または設定可能にすることも考えられる。この場合には、ＷＷＷサーバ１が設置されているネットワーク環境に応じた設定ができるようになり、非常に汎用性の高いものとなる。

【００５３】また、本実施の形態では、認証期限データ内にエントリが存在しているか否かを「操作者名」および「ＩＰアドレス」に基づいて判断する場合について説明したが、本発明はこれに限定されるものではない。例えば「操作者名」と「ＩＰアドレス」とのいずれか一方のみに基づいて判断したり、あるいはこれら以外の情報で利用者端末（または利用者）を識別するためのものに基づいて判断することも実現可能である。

【００５４】

【発明の効果】以上に説明したように、本発明の画像処理装置は、処理要求の発行元である外部装置に応じて決定すべき有効期間の長さを変化させるようになっているので、処理要求の発行元に応じた認証の重み付けをすることが可能となる。したがって、この画像処理装置によれば、例えばこの画像処理装置とは遠い環境条件の外部装置に対してはそのセキュリティを確保しつつ、近い環境条件の外部装置に対しては処理効率や操作性の悪化を防ぐことができるようになる。つまり、処理要求の発行元の特性（環境や性能等）に応じて認証期限を自動的に決定することで、処理要求の発行元となる外部装置側での操作性を損なうことなく、提供するサービスのセキュリティを確保することができるという効果を奏する。

【図面の簡単な説明】

【図１】　本発明に係る画像処理装置にて認証処理を行う場合における処理手順の一例を示すフローチャートである。

【図２】　本発明を適用したＷＷＷサーバの概略構成の一例を示すブロック図である。

【図３】　認証処理を行う場合に用いる利用者データの具体例を示す説明図である。

【図４】　認証処理を行う場合に用いる認証期限データの具体例を示す説明図である。

【図５】　ＢＡＳＩＣ認証を行った際のＷＷＷサーバと

11

利用者端末との間のデータ授受の概要を示す説明図である。

【図６】　ＨＴＴＰプロトコルによる情報要求時における授受データの具体例を示す説明図である。

【図７】　ＨＴＴＰプロトコルによる情報応答時（要認証時）における授受データの具体例を示す説明図である。

【図８】　ＨＴＴＰプロトコルによる個人情報通知時における授受データの具体例を示す説明図である。

【図９】　ＨＴＴＰプロトコルによる情報応答時（認証成功時）における授受データの具体例を示す説明図である。

12

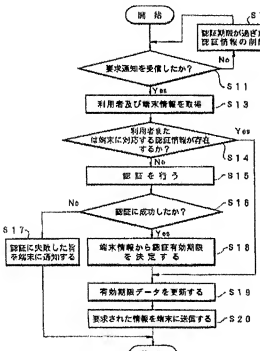
【図１０】　ＨＴＴＰプロトコルによる情報応答時（認証失敗時）における授受データの具体例を示す説明図である。

【図１１】　認証処理の結果に対する有効期限を決定する際の算出方法の一例を示す説明図である。

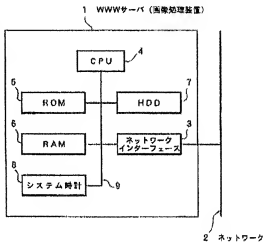
【符号の説明】

１…ＷＷＷサーバ（画像処理装置）、２…ネットワーク、３…ネットワークインタフェース、４…ＣＰＵ、５…ＲＯＭ、６…ＲＡＭ、７…ハードディスク装置（ＨＤＤ）、８…システム時計

【図１】



【図２】



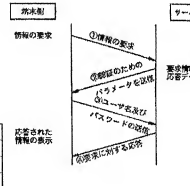
【図３】

操作者名	パスワード
suzuki	abc012
tanaka	ghi345
sato	jkl678
takahashi	mno901
tanaka	ghi346

【図４】

操作者名	ＩＰアドレス	認証有効期限
suzuki	129.249.**.21	Wed,28 May1999 19:10:21
tanaka	129.249.**.30	Wed,28 May1999 11:00:50
sato	129.249.**.21	Wed,28 May1999 09:21:31
takahashi	129.249.**.43	Wed,28 May1999 15:45:22
tanaka	129.125.**.10	Wed,28 May1999 09:20:00

【図５】



【図７】

```
HTTP/1.0 401 Unauthorized
Last-Modified: Thu, 04 Jun 1998 00:00:02 JST
Expires: Fri, 05 Jun 1999 00:00:04 JST
Content-Type: text/html
WWW-Authenticate:Basic realm="SECRET_PAGE"
（以下データ列）
```

【図６】

```
GET /Secure/secure.htm HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: ja
Accept-Encoding:gzip, deflate
User-Agent: Mozilla/4.0 (compatible)
Host:www.fujixerox.co.jp
From:eeeee@bbb.ccc.co.jp
Proxy-Connection: Keep-Alive
```

【図８】

```
GET /Secure/secure.htm HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: ja
Accept-Encoding:gzip, deflate
User-Agent: Mozilla/4.0 (compatible)
Host:www.fujixerox.co.jp
From:eeeee@bbb.ccc.co.jp
Proxy-Connection: Keep-Alive
Authorization:Basic SGlyYW1lEdvbNEgR2SrYO=
```

【図９】

```
HTTP/1.0 200 OK
Last-Modified: Thu, 04 Jun 1999 00:00:02 JST
Expires: Fri, 05 Jun 1999 00:00:04 JST
Content-Type: text/html

(以下データ列)
```

【図１０】

```
HTTP/1.0 403 Forbidden
Last-Modified: Thu, 04 Jun 1999 00:00:02 JST
Expires: Fri, 05 Jun 1999 00:00:04 JST
Content-Type: text/html

(以下データ列)
```

【図１１】

有効期限＝現在時刻＋有効期間　　……（１）
有効期間＝最大有効期間×有効期間係数　　……（２）
最大有効期間＝１日＝24時間＝1440分　　……（３）

一致対象アドレス：

- 128.249.10.1
- 128.246.21.11
- 128.212.41.8

一致しているアドレス桁（上位より）	一致しているアドレス初（XXX=一致している数字、ooo=一致していない数字）	有効期限係数
１２桁	XXX.XXX.XXX.XXX	1
１１桁から９桁	XXX.XXX.XXX.ooo	0.7
８桁から６桁	XXX.XXX.ooo.ooo	0.5
５桁から３桁	XXX.ooo.ooo.ooo	0.2
２桁以下	ooo.ooo.ooo.ooo	0